

ABSTRACT

A digital signature is generated in association with target data. The computer generating the digital data encrypts the digital signature using a public key encryption system. The private key is stored in dynamic memory in a secure manner. The public key associated with the private key is stored in an accessible database. The public key is accessed from the database and used by recipient computers to authenticate the target data by decrypting the encrypted digital signature. When the computer generating the digital signature is restarted, the private key stored in dynamic memory is lost. The computer obtains a new private and public key pair from the public key encryption system. The previously used public key is maintained in the database until a predefined time has elapsed, after which it is removed from the database.

[illegible]